Have a safe Christmas...

online and offline

GET SAFE ONLINE .org

www.getsafeonline.org

Having a safe online Christmas is about more than just shopping.

As if you needed reminding, Christmas is just around the corner. However, you may still have gifts, decorations and other festive items to buy before the big day. With the COVID-19 pandemic still very much with us, shopping on the internet may well be your preferred choice, making it very important to make sure you're buying safely and securely, and not falling victim to a scam.

But a safe online Christmas is also about far more than shopping: it's how you set up and use those new connected devices, make sure the young people in your life are going online safely and responsibly and remain vigilant when there's so much going on around you, including keeping yourself and the family protected from the virus.

This year, it may also be more difficult to physically get together with loved ones and friends, so you'll also need to take care when connecting with them online.

#onlinechristmas

We've put together some expert tips to help you get through this year's festive season online with safety, security and confidence.

Online shopping

Make sure you can spot the difference between genuine and **fake websites**, secure and **insecure payment pages** and authentic and **counterfeit goods**. You can find more information at **www.getsafeonline.org/safechristmas**

Scams

Fraudsters love the festive season, using the opportunity to send fake links in emails, texts and posts, or even email attachments posing as Christmas parcel delivery notifications. They could also call you claiming to be from your bank, a retailer, a delivery firm or software support company, but with one aim – stealing your money or identity. If in any doubt, always call the organisation on the number you know to be correct.

Phones, tablets & computers

Protect all new or second-hand internet-connected phones, tablets and computers with a **reputable security app/software**. Some suppliers offer a single solution that protects multiple devices. Add a **PIN or passcode** as soon as you power up. Ensure all devices are **regularly backed up** so you don't lose your valuable documents and other files, or those precious photos.

Software, operating system and app updates

Download updates to operating systems, apps and software as soon as you're notified that they're available. If you don't, you risk devices being infected by malware, and possible fraud or identity theft. Better still, set them to update automatically.

Mobile apps

Download apps only from official sources such as App Store, Google Play or Microsoft Store. Apps from unofficial sources could result in fraud or identity theft.

Smart devices & wearables

To improve security, **passwords on internet-connected devices** like voice assistants, CCTV cameras, appliances, kids' toys and fitness watches should be changed from the factory default as soon as you unpack and switch them on. Always use different passwords for different devices, websites or accounts to avoid them being hacked. Be careful what you say within hearing distance of **voice assistants** as you can't be sure what conversations they're picking up.

Gaming

With new consoles and games coming out this year – and continued use of existing ones – remember to stay safe and secure, including avoiding oversharing, griefing, overspending on in-game properties and pirated games. Don't lose track of how much time you're spending online. Pass on this advice to your children too, including what interactions they're having with strangers.

Second-hand mobile devices

If you're selling or gifting a computer or mobile device, **perform a factory reset** to erase your data. You can find out how from the manufacturer's website. If you've bought or been given a pre-owned device, remove the previous owner's settings and data if this hasn't already been done.

Out & about with your mobile devices

Wi-Fi hotspots in cafés, pubs, hotel rooms, on public transport or other public areas may not be secure. They may also be fake, set up by a fraudster. For this reason, avoid connecting with them if you're doing anything confidential online. Keep devices themselves protected from theft or loss. Be wary of people watching your screen over your shoulder.

Avoid oversharing

Stop and ask yourself if **what you're about to share on social media** is really necessary. Could it be helping a fraudster? Could it give your children a digital footprint they don't want? Posting about being away could be telling a burglar that your home is empty. And why not take a few minutes over Christmas to review your **privacy settings**?

Safeguarding children

Help the children and young people in your life to protect themselves. **Have the talk about safe and responsible internet use**, including what they share, who they're communicating with and the type of content they access, including apps and games. Consider downloading a respected parental control app and using ISP filters to block unsuitable content. Make sure your children aren't running up bills for in-app or in-game purchases.

Video calls

This year, many of us will be catching up via a video call. Apart from using a service that everyone finds easy to use, **make sure it's secure** by choosing one that needs a strong password, and don't share the call invitation or details outside the group on the call.

For more information on how to stay safe online this festive season, visit www.getsafeonline.org/onlinechristmas

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you've been a victim of online fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre on 0300 123 20 40 or at www.actionfraud.police.uk

In Scotland, report fraud to Police Scotland by calling 101.

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO · kaspersky · Gumtree · Standard Life · first direct · M&S BANK · HSBC · Royal Bank of Scotland · NatWest · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ROYAL AIR FORCE · CITY of LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VS VICTIM SUPPORT · EUROPOL EC3 · ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT